Exhibit 16

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, DC 20549

FORM 8-K

CURRENT REPORT

**PURSUANT TO SECTION 13 OR 15(d) OF
THE SECURITIES EXCHANGE ACT OF 1934**

**May 7, 2021
Date of Report (Date of earliest event reported)**

SOLARWINDS CORPORATION
(Exact name of registrant as specified in its charter)

Delaware	**001-38711**	**81-0753267**
(State or other jurisdiction of incorporation)	**(Commission File Number)**	**(IRS Employer Identification No.)**

**7171 Southwest Parkway
Building 400
Austin, Texas 78735
(Address of principal executive offices) (Zip Code)**

Registrant's telephone number, including area code: (512) 682-9300

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instruction A.2. below):

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	Trading Symbol	Name of Each Exchange on Which Registered
Common Stock, $0.001 par value	SWI	New York Stock Exchange

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 7.01 Regulation FD Disclosure.

On May 7, 2021, SolarWinds Corporation ("***SolarWinds***" or the "***Company***") provided the following update on the cyberattack announced in December 2020, or the Cyber Incident, on its Orange Matter blog, accessible at https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack:

An Investigative Update of the Cyberattack

The recent cyberattacks against SolarWinds, other widely used technology providers, and our respective customers are examples of the ongoing challenges facing the software industry as a whole. It's clear that nation-state actors are actively working to compromise and disrupt the technology supply chains and infrastructure on which we all rely.

Throughout this experience, we've emphasized transparency, collaboration with our public and private partners, and knowledge-sharing from our investigations as information is gathered and verified. Over the past five months, we've devoted extensive resources to investigating this cyber attack and working with experts to sift through terabytes of data. We've been determined to uncover the tools, tactics, and motives of the nation-state threat actor to better protect SolarWinds, our customers, and others in the future.

We're close to completing these extensive investigative efforts with assistance from our third-party experts and would like to provide another update on what we've learned to supplement our prior posts.

Our Awareness of Impact to Customers

We also want to take a moment to discuss our understanding about the impact of this attack on our customers. Our attitude will continue to be: one customer impacted is one customer too many.

We've worked tirelessly to support our customers and to contain, eradicate, and remediate the cyber incident. We quickly published information about the attack and notified our customers. We also released remediations to the affected versions of the Orion Platform software and engaged in extensive outreach and support to our customers. We also made available third-party support at our expense to help customers upgrade their Orion Platform software.

Through our numerous blog posts, webinars, TechPod podcasts, interviews, and other public statements, we've provided to our customers, and to the industry more broadly, substantial information about the cyber incident and our learnings and adaptation from it to help them better understand the attack and protect themselves.

Based on our investigations and conversations with our customers, we believe the number of customers targeted and impacted by the SUNBURST malicious code is significantly fewer than the number of potentially vulnerable customers. At the earliest stages of our investigation, we reported up to 18,000 customers *could* potentially have been vulnerable to SUNBURST, based on our records of the total number of customer downloads of the specific, impacted versions of our Orion Platform products. Unfortunately, we've seen this number used mistakenly in media reports as the number of customers that the threat actor *actually* hacked through SUNBURST.

We now estimate that the actual number of customers who were hacked through SUNBURST to be fewer than 100. It's important to note that this group of up to 18,000 downloads includes two significant groups that could not have been affected by SUNBURST due to the inability of the malicious code to contact the threat actor command-and-control server: (1) those customers who did not install the downloaded version and (2) those customers who did install the affected version, but only did so on a server *without* access to the internet. Among a third group of customers, those whose affected servers accessed the internet, we believe, based on sample DNS data, only a very small proportion saw any activity with the command-and-control server deployed by the threat actor. This statistical analysis of the same DNS data leads to our belief that fewer than 100 customers had servers that communicated with the threat actor. This information is consistent with estimates provided by U.S. government entities and other researchers, and consistent with the presumption the attack was highly targeted.

Orion Platform Supply-Chain Attack

Most of our early investigative efforts focused on the compromise of our Orion Platform software products and understanding the nature of the attack. It became clear early on the threat actor employed novel and sophisticated techniques indicative of a nation-state actor and consistent with the goal of cyber espionage via a supply-chain attack. In addition, the operational security of the threat actor was so advanced, they not only attacked SolarWinds but were able to leverage the SUNBURST malicious code and avoid detection in some of the most complex environments in the world.

During the course of our investigations, we discovered the following:

•The threat actor *did not* modify our source code repository. The malicious activity occurred within the automated build environment for our Orion Platform software. Through the use of the novel SUNSPOT code injector that we discovered in our investigation, the threat actor surreptitiously injected the SUNBURST malicious code solely into builds of the Orion Software Platform. We published details about the build manipulation activity in our January 11 blog post, and with our investigative partner CrowdStrike, published extensive information about SUNSPOT to help others in the industry protect themselves against its use in their environments.
• The threat actor undertook a test run of its ability to inject code into builds of the Orion Software Platform software in October 2019, months prior to initiating the actual SUNBURST injection into builds of our Orion Software Platform released between March and June 2020.
• We have not identified SUNBURST in any of our more than 70 non-Orion Platform products and tools, including those of our N-able business.

Shared IT Environment Activities
We narrowed it down to three most likely candidates for initial entry, but we don't limit the methods to these three. This excludes the possibility the initial access was through a known, unpatched vulnerability:

- Zero-day vulnerability in a third-party application or device;
- Brute-force attack, such as a password spray attack; or
- Social engineering, such as a targeted phishing attack.

While we don't know precisely when or how the threat actor first gained access to our environment, our investigations have uncovered evidence that the threat actor compromised credentials and conducted research and surveillance in furtherance of its objectives through persistent access to our software development environment and internal systems, including our Microsoft Office 365 environment, for at least nine months prior to initiating the test run in October 2019. Based on our learnings, while unfortunate, it's not uncommon for threat actors to be in target environments for several months to years. This further reinforces the need for transparency and collaboration, so we can all benefit from one another's shared experiences and knowledge.

We've also found evidence that causes us to believe the threat actor exfiltrated certain information as part of its research and surveillance. This evidence includes the following:

• The threat actor created and moved files that we believe contained source code for both Orion Platform software and non-Orion products. However, we are unable to determine the actual contents of those files.
• The threat actor created and moved additional files, including a file that may have contained data supporting our customer portal application. Although we're unable to determine the actual contents of the files, the information included in our customer portal databases does not contain highly sensitive personal information, such as credit card, Social Security, passport details, or bank account numbers, but contains other information such as corporate customer name, business email addresses, business billing addresses, encrypted portal login credentials, IP addresses downloading any software and MAC addresses of the registered Orion servers.
• The threat actor accessed email accounts of certain personnel, some of which contained information related to current or former employees and customers. We are currently in the process of identifying all personal information contained in the emails of these accounts and expect to provide notices to any impacted individuals and other parties as appropriate.
• The threat actor moved files to a jump server, which we believe was intended to facilitate exfiltration of the files out of our environment.

Our Remediation Activities
Together with our partners KPMG and CrowdStrike, in conjunction with government agencies, we've undertaken extensive measures to investigate, contain, eradicate, and remediate the cyber incident. CrowdStrike performed a macro-level analysis of the SolarWinds environment and deployed their Falcon technology and other threat-hunting tools, providing ongoing monitoring for suspicious activity. The KPMG forensics team performed micro-level analysis, conducting deep inspections of our build environments, as well as additional forensics and analysis. This analysis included inspection of various artifacts, including historical firewall logs, access control logs, and SIEM events. At this time, we've substantially completed this process and believe the threat actor is no longer active in our environments.

Our Future: Secure by Design
Armed with what we've learned about this attack, we're focused on becoming an industry leader in protecting our software development from cyberintrusions. We're working with industry experts to implement enhanced security practices designed to further strengthen and protect our products and environment against these and other types of attacks in the future. To that end, we're further securing our environment and systems by:

- Upgrading to stronger and deeper endpoint protections within our environment;
- Enhancing our Data Loss Prevention solution to better detect low and slow leaks;
- Expanding our Security Operations Center to improve visibility and threat hunting across our network; and
- Tightening our firewall policies to further limit east/west traffic.

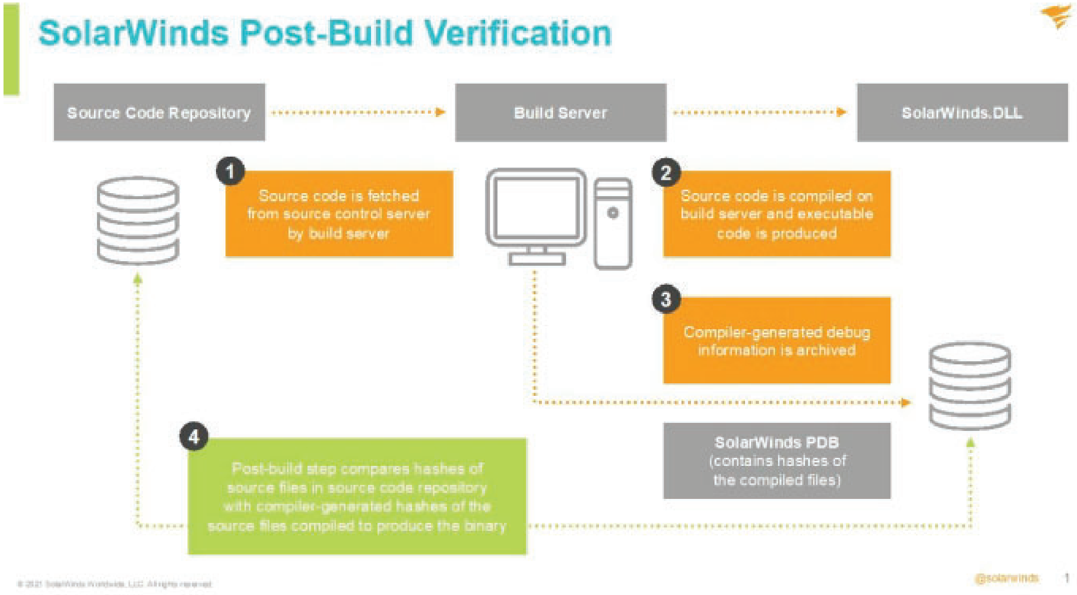
Additionally, we're adopting zero trust and least privilege access mechanisms by:

- Expanding and more consistently enforcing least privileges policies for ALL employees;
- Limiting external interfaces to our environments; and
- Increasing, expanding, and strictly enforcing requirements for multi-factor authentication throughout our environment, as well as expanding the use of a privilege access manager for all administrative accounts, with auditing.

Further, we're addressing the possible risks associated with third-party applications access by:

- Increasing on-going monitoring and inspection of all SaaS tools within our environment;
- Ensuring that the configurations and implementation of all tools within our environment align with best practices;
- Reviewing all accounts, updating all passwords and turning up the level of conditional access; and
- Strengthening the level of pre-procurement security reviews for all vendors.

Additionally, we have made significant progress in redesigning our automated build process to help ensure the security and integrity of the code our products and that no insertions or alterations have occurred during the build process as occurred happened with SUNSPOT and SUNBURST. The below illustration illustrates highlights how this new build process works:



SolarWinds Post-Build Verification

Source Code Repository

Build Server

SolarWinds.DLL

1 Source code is fetched from source control server by build server

2 Source code is compiled on build server and executable code is produced

3 Compiler-generated debug information is archived

SolarWinds PDB (contains hashes of the compiled files)

4 Post-build step compares hashes of source files in source code repository with compiler-generated hashes of the source files compiled to produce the binary

@solarwinds 1

In addition to these protective steps, we're conducting our software builds in three separate environments, using changing build systems, and with separate user credentials. We check the integrity of the builds across these environments to identify and address any compromises. In this way, we are changing and shifting the threat surface, thereby forcing a threat actor to replicate an attack across multiple heterogeneous environments with no overlapping privileges to be successful.

We use a standard Secure Development lifecycle approach. That includes requirements analysis, secure development, security testing, release and respond. As part of the process Checkmarx is utilized for static code analysis, Whitesource is utilized for Open-Source discovery/analysis, and internal PEN testing utilizing Burpsuite prior to a final security review.

In addition to the build pipeline, business critical assets are identified, tracked, and reviewed on a regular basis. Security controls are defined for each asset.

We hope sharing of our learnings about this attack serves our customers - as well as the broader IT industry - given the common development practices in the industry and our belief that transparency and cooperation are our industry's best tools to help prevent and protect against future attacks. We also believe it illustrates the lengths to which outside nation-states will go to achieve their malicious goals and the need for the industry and public sector to work together to protect critical systems and infrastructure. We see an opportunity to help lead an industry-wide effort we believe will position SolarWinds as a model for secure software environments, development processes, and products.

We see these as initiatives and investments as being consistent with our goal of being a best-in-class provider of powerful, affordable, and secure solutions.

This Blog Post contains "forward-looking" statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995, including statements regarding SolarWinds' investigation of the recent cyber incident (the "Cyber Incident"), the company's findings to date, SolarWinds' understanding of the nature, source and duration of the attack, including the threat actor's access to SolarWinds environment, SolarWinds understanding of any confidential, proprietary or personal information, including of SolarWinds' current or former employees and customers, that may have been accessed and exfiltrated by the threat actor, SolarWinds' plans to identify all personal information contained in emails that were accessed by the threat actor and to provide notices to any impacted individuals, and SolarWinds' plans to further enhance our security practices. The information in this Blog Post is based on management's beliefs and assumptions and on information currently available to management, which may change as SolarWinds continues to address and investigate the Cyber Incident and related matters and if new or different information is discovered about these matters or generally. Forward-looking statements include all statements that are not historical facts and may be identified by terms such as "aim," "anticipate," "believe," "can," "could," "seek," "should," "feel," "expect," "will," "would," "plan," "intend," "estimate," "continue," "may," or similar expressions and the negatives of those terms. Forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause actual results, performance or achievements to be materially different from any future results, performance or achievements expressed or implied by the forward-looking statements. Factors that could cause or contribute to such differences include, but are not limited to, (a) the discovery of new or different information regarding the Cyber Incident, including with respect to its scope, the threat actor's access to our environment and its related activities during such period, and the related impact on our systems, products, current or former employees and customers, (b) the possibility that our mitigation and remediation efforts with respect to the Cyber Incident may not be successful, (c) the possibility that additional confidential, proprietary or personal information, including information of SolarWinds' current or former employees and customers, was accessed and exfiltrated as a result of the Cyber Incident, (d) numerous financial, legal, reputational and other risks to us related to the Cyber Incident, including risks that the incident or SolarWinds' response thereto, including with respect to providing notices to any impacted individuals, may result in the loss, compromise or corruption of data and proprietary information, loss of business as a result of termination or non-renewal of agreements or reduced purchases or upgrades of our products, severe reputational damage adversely affecting customer, partner and vendor relationships and investor confidence, increased attrition of personnel and distraction of key and other personnel, U.S. or foreign regulatory investigations and enforcement actions, litigation, indemnity obligations, damages for contractual breach, penalties for violation of applicable laws or regulations, significant costs for remediation and the incurrence of other liabilities, (e) risks that our insurance coverage, including coverage relating to certain security and privacy damages and claim expenses, may not be available or sufficient to compensate for all liabilities we incur related to these matters, (f) the possibility that our steps to secure our internal environment, improve our product development environment and protect the security and integrity of the software that we deliver to our customers may not be successful or sufficient to protect against future threat actors or attacks or perceived by existing and prospective customers as sufficient to address the harm caused by the Cyber Incident, and (g) such other risks and uncertainties described more fully in documents filed with or furnished to the U.S. Securities and Exchange Commission by SolarWinds, including the risk factors discussed in SolarWinds' Annual Report on Form 10-K for the period ended December 31, 2020 filed on March 1, 2021. All information provided in this Blog Post is as of the date hereof and SolarWinds undertakes no duty to update this information except as required by law.

* * *

The information contained in this Current Report on Form 8-K pursuant to this "Item 7.01 Regulation FD Disclosure" shall not be deemed "filed" for purposes of Section 18 of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), or otherwise subject to the liability of that section. The information in this section of this Current Report on Form 8-K shall not be incorporated by reference in any filing under the Securities Act of 1933, as amended, or the Exchange Act except as shall be expressly set forth by specific reference in such a filing.

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

SOLARWINDS CORPORATION

Dated:	May 7, 2021	By:	/s/ Sudhakar Ramakrishna *Sudhakar Ramakrishna* *President and Chief Executive Officer*

Cover - COVER PAGE COVER PAGE

COVER PAGE COVER PAGE	XBRL Tag Name	XBRL Prefix	Data Type	Balance Type	Period Type	May 07, 2021
Cover [Abstract]	dei_CoverAbstract	dei_	xbrli:stringItemType	na	duration	
Document Type	dei_DocumentType	dei_	dei:submissionTypeItemType	na	duration	8-K
Document Period End Date	dei_DocumentPeriodEndDate	dei_	xbrli:dateItemType	na	duration	May 07, 2021
Entity Registrant Name	dei_EntityRegistrantName	dei_	xbrli:normalizedStringItemType	na	duration	SOLARWINDS CORP
Entity Incorporation, State or Country Code	dei_EntityIncorporationStateCountryCode	dei_	dei:edgarStateCountryItemType	na	duration	DE
Entity File Number	dei_EntityFileNumber	dei_	dei:fileNumberItemType	na	duration	001-38711
Entity Tax Identification Number	dei_EntityTaxIdentificationNumber	dei_	dei:employerIdItemType	na	duration	81-0753267
Entity Address, Address Line One	dei_EntityAddressAddressLine1	dei_	xbrli:normalizedStringItemType	na	duration	7171 Southwest Parkway
Entity Address, Address Line Two	dei_EntityAddressAddressLine2	dei_	xbrli:normalizedStringItemType	na	duration	Building 400
Entity Address, City or Town	dei_EntityAddressCityOrTown	dei_	xbrli:normalizedStringItemType	na	duration	Austin
Entity Address, State or Province	dei_EntityAddressStateOrProvince	dei_	dei:stateOrProvinceItemType	na	duration	TX
Entity Address, Postal Zip Code	dei_EntityAddressPostalZipCode	dei_	xbrli:normalizedStringItemType	na	duration	78735
City Area Code	dei_CityAreaCode	dei_	xbrli:normalizedStringItemType	na	duration	512
Local Phone Number	dei_LocalPhoneNumber	dei_	xbrli:normalizedStringItemType	na	duration	682-9300
Title of 12(b) Security	dei_Security12bTitle	dei_	dei:securityTitleItemType	na	duration	Common Stock, $0.001 par value
Trading Symbol	dei_TradingSymbol	dei_	dei:tradingSymbolItemType	na	duration	SWI
Security Exchange Name	dei_SecurityExchangeName	dei_	dei:edgarExchangeCodeItemType	na	duration	NYSE
Written Communications	dei_WrittenCommunications	dei_	xbrli:booleanItemType	na	duration	false
Soliciting Material	dei_SolicitingMaterial	dei_	xbrli:booleanItemType	na	duration	false
Pre-commencement Tender Offer	dei_PreCommencementTenderOffer	dei_	xbrli:booleanItemType	na	duration	false
Pre-commencement Issuer Tender Offer	dei_PreCommencementIssuerTenderOffer	dei_	xbrli:booleanItemType	na	duration	false
Entity Emerging Growth Company	dei_EntityEmergingGrowthCompany	dei_	xbrli:booleanItemType	na	duration	false
Entity Central Index Key	dei_EntityCentralIndexKey	dei_	dei:centralIndexKeyItemType	na	duration	0001739942
Amendment Flag	dei_AmendmentFlag	dei_	xbrli:booleanItemType	na	duration	false

+ References + Details